

POWERED BY **Dialog**

---

**READ-OUT DEVICE FOR RECORDING MEDIUM AND DATA PROCESSING DEVICE****Publication Number:** 11-250568 (JP 11250568 A) , September 17, 1999**Inventors:**MORI MASAHIRO  
NAKAMURA TADASHI**Applicants**

SONY CORP

**Application Number:** 10-045846 (JP 9845846) , February 26, 1998**International Class:**

G11B-020/10

**Abstract:**

PROBLEM TO BE SOLVED: To provide a read-out device for an optical disk recording medium in which processing burden of a microcomputer can be lightened, in a DVD-ROM drive device. SOLUTION: Key data 22a, 22b recorded in a DVD disk 10 and contents data 21a of which utilization is controlled by the key data are read out, read out key data 20a, 20b are ciphered by an authentication section 140, and the ciphered key data 20a, 20b and read out contents data 21a are transmitted to the outside through an interface 42. In the authentication section 140, data transfer accompanied by ciphering processing is controlled by a DMA section provided independently of the microcomputer performing servo control of rotation of the DVD disk and the like. COPYRIGHT: (C)1999,JPO

JAPIO

© 2001 Japan Patent Information Organization. All rights reserved.  
Dialog® File Number 347 Accession Number 6308971

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-250568

(43) 公開日 平成11年(1999) 9月17日

(51) Int.Cl.<sup>6</sup>

識別記号

F I

G 1 1 B 20/10

G 1 1 B 20/10

H

審査請求 未請求 請求項の数15 O L (全 9 頁)

(21) 出願番号 特願平10-45846  
(22) 出願日 平成10年(1998) 2月26日

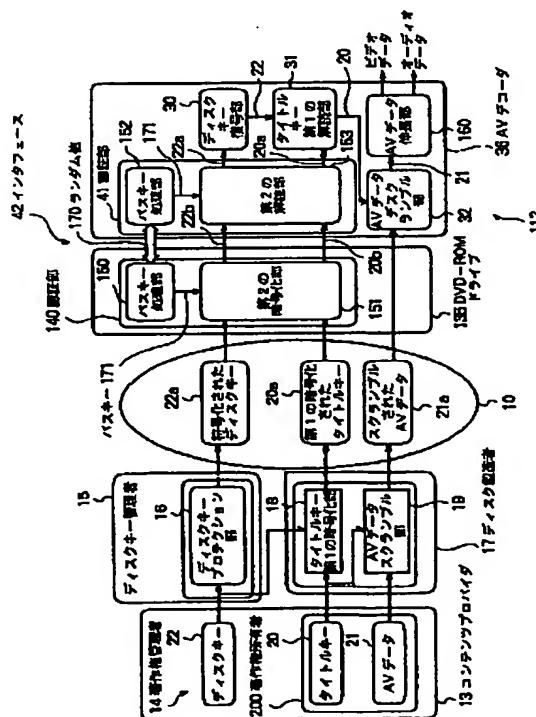
(71) 出願人 000002185  
ソニー株式会社  
東京都品川区北品川6丁目7番35号  
(72) 発明者 森 雅弘  
東京都品川区北品川6丁目7番35号 ソニ  
ー株式会社内  
(72) 発明者 中村 忠  
東京都品川区北品川6丁目7番35号 ソニ  
ー株式会社内  
(74) 代理人 弁理士 佐藤 隆久

(54) 【発明の名称】 記録媒体読み出し装置およびデータ処理装置

(57) 【要約】

【課題】 DVD-ROMドライブ装置において、マイクロコンピュータの処理負担を軽減できる光ディスク記録媒体読み出し装置を提供する。

【解決手段】 DVDディスク10に記録された鍵データ22a、20aと当該鍵データによって利用が管理されるコンテンツデータ21aとを読み出し、読み出した鍵データ20a、22bを認証部140で暗号化し、当該暗号化された鍵データ20a、22bと読み出したコンテンツデータ21aとを、インタフェース42を介して外部に伝送する。認証部140では、DVDディスクの回転などのサーボ制御を行うマイクロコンピュータとは別に設けられたDMA部によって、暗号化処理に伴うデータ転送が制御される。



## 【特許請求の範囲】

【請求項1】記録媒体に記録された鍵データと当該鍵データによって利用が管理されるコンテンツデータとを読み出し、前記読み出した鍵データを暗号化し、当該暗号化された鍵データを前記読み出したコンテンツデータと共に、インタフェースを介して外部に伝送する記録媒体読み出し装置において、

少なくとも前記記録媒体から前記鍵データおよび前記コンテンツデータを読み出す制御を含む、当該記録媒体読み出し装置における制御を統括的に行う第1の制御手段と、

前記読み出した鍵データおよび前記コンテンツデータを記憶する記憶手段と、

前記記憶手段に記憶された前記鍵データを暗号化する暗号化手段と、

前記記憶手段と前記暗号化手段との間の前記鍵データの転送を制御し、前記第1の制御手段とは別個に設けられた第2の制御手段とを有する記録媒体読み出し装置。

【請求項2】前記第1の制御手段、前記記憶手段、前記暗号化手段、前記第2の制御手段および前記インタフェースは、内部バスを介して接続してある請求項1に記載の記録媒体読み出し装置。

【請求項3】前記暗号化手段は、自らが生成したランダムデータと、前記インタフェースを介して入力したランダムデータとに基づいて、前記鍵データを暗号化する請求項1に記載の記録媒体読み出し装置。

【請求項4】前記第1の制御手段は、前記第2の制御手段に、暗号化処理の開始を指示する請求項1に記載の記録媒体読み出し装置。

【請求項5】前記第2の制御手段は、ダイレクトメモリアクセス方式を用いている請求項1に記載の記録媒体読み出し装置。

【請求項6】前記記録媒体は、光ディスク記録媒体である請求項1に記載の記録媒体読み出し装置。

【請求項7】前記コンテンツデータは、映像データである請求項1に記載の記録媒体読み出し装置。

【請求項8】前記コンテンツデータは、映像データおよび音響データである請求項1に記載の記録媒体読み出し装置。

【請求項9】記録媒体から読み出され、暗号化された鍵データと当該鍵データによって利用が管理されるコンテンツデータとを、インタフェースを介して、記録媒体読み出し装置からデコーダ装置に伝送するデータ処理装置において、

前記記録媒体読み出し装置は、

少なくとも前記記録媒体から前記鍵データおよび前記コンテンツデータを読み出す制御を含む、当該記録媒体読み出し装置における制御を統括的に行う第1の制御手段と、

前記読み出した鍵データおよび前記コンテンツデータを

記憶する記憶手段と、

自らが生成した第1のランダムデータと、前記インタフェースを介して前記デコーダ装置から入力した第2のランダムデータに基づいて、前記記憶手段に記憶された前記鍵データを暗号化する暗号化手段と、

前記記憶手段と前記暗号化手段との間の前記鍵データの転送を制御し、前記第1の制御手段とは別個に設けられた第2の制御手段とを有し、

前記デコーダ装置は、

前記インタフェースを介して前記記録媒体読み出し装置から入力した前記第1のランダムデータと、自らが生成した前記第2のランダムデータとに基づいて、前記インタフェースを介して入力した前記暗号化された鍵データを解読する解読手段と、

前記解読された鍵データを用いて、前記インタフェースを介して入力したコンテンツデータを利用可能にするコンテンツデータ処理手段とを有するデータ処理装置。

【請求項10】前記記録媒体読み出し装置では、前記第1の制御手段、前記記憶手段、前記暗号化手段、前記第2の制御手段および前記インタフェースは、内部バスを介して接続してある請求項9に記載のデータ処理装置。

【請求項11】前記第2の制御手段は、ダイレクトメモリアクセス方式を用いている請求項9に記載のデータ処理装置。

【請求項12】前記記録媒体は、光ディスク記録媒体である請求項9に記載のデータ処理装置。

【請求項13】前記コンテンツデータは、映像データである請求項9に記載のデータ処理装置。

【請求項14】前記コンテンツデータは、映像データおよび音響データである請求項9に記載のデータ処理装置。

【請求項15】前記第1の制御手段は、前記第2の制御手段に、暗号化処理の開始を指示する請求項9に記載のデータ処理装置。

## 【発明の詳細な説明】

## 【0001】

【発明が属する技術分野】本発明は、DVDディスクなどの記録媒体に記録されたデータの読み出しを行う記録媒体読み出し装置およびデータ処理装置に関する。

## 【0002】

【従来の技術】近年、DVD(Digital Video Disc)プレーヤや、DVD-ROM(Read Only Memory)装置用のLSIが活発に開発されている。DVDには、著作権保護の観点から、所定のアルゴリズムで符号化されたディスクキーと、暗号化(Encryption)されたタイトルキーとが記録されており、DVDプレーヤおよびコンピュータなどは、これら符号化されたディスクキーおよび暗号化されたタイトルキーを、それぞれ復号および解読しないと、記録されたAVデータ(コンテンツデータ)に利用できないようになっている。ここで、ディスクキーは、

例えば、1枚のDVDディスクに1つ記録され、これを復号したときにのみ、DVDディスクに記録された他のデータの利用が許可される。また、タイトルキーは、DVDディスクに記録された複数のコンテンツのそれぞれに設けられ、復号されたタイトルキーに対応するコンテンツのAVデータのみ利用が許可される。

【0003】図4は、DVDディスク10へのディスクキーおよびタイトルキーの記録から、DVDディスク10に記録されたAVデータをDVDプレーヤ11およびコンピュータ（DVD-ROMドライブ装置）12を用いて再生するまでの過程を説明するための図である。図4に示すように、コンテンツプロバイダ13の一人である著作権所有者200が、著作権の対象となるAVデータ21と、発行したタイトルキー20とをディスク製造者17に供給する。また、コンテンツプロバイダ13の一人である著作権管理者14が、ディスクキー22を発行し、これをディスクキー管理者15に供給する。ディスクキー管理者15は、ディスクキープロテクション部16において、ディスクキー22を符号化する。この符号化されたディスクキー22aは、DVDディスク10に記録される。

【0004】ディスク製造者17は、タイトルキー暗号化部18でタイトルキー20の第1の暗号化を行うと共に、AVデータ21をAVデータスクランブル部19でタイトルキー20を用いてスクランブル(Scramble)する。また、ディスク製造者17は、第1の暗号化されたタイトルキーと、スクランブルされたAVデータと、ディスクキー管理者15からの符号化されたディスクキー22aとを記録したDVDディスク10を製造する。

【0005】DVDディスク10は、出荷された後に、例えば、ユーザのDVDプレーヤ11にセットされる。DVDプレーヤ11は、再生動作において、まず、ディスクキー復号部30で、符号化されたディスクキー22aを復号し、当該復号が成功すると、次に、当該復号されたディスクキーを用いて、ユーザから指示のあったコンテンツに対応するタイトルキーをタイトルキー解読部31で解読し、当該解読に成功すると、次に、当該タイトルキーを用いて、対応するAVデータをデスクランブル部32でデスクランブル(Descramble)して、AVデータS11としてディスプレイ33に出力する。

【0006】また、コンピュータ12には、DVD-ROMドライブ35およびAVデコーダ36が設けられている。DVD-ROMドライブ35とAVデコーダ36とは、例えば、ATAPI(AT Attachment Packet Interface)あるいはSCSI(Small Computer System Interface)などのインタフェース42を介して接続されている。DVD-ROMドライブ35には認証部(Authentication)40が設けられている。DVD-ROMドライブ35では、インタフェース42を介して伝送する鍵データに対して、認証部40で所定の暗号化を行うことが、

規格によって決められている。また、AVデコーダ36には、認証部41、ディスクキー復号部30、タイトルキー解読部31およびAVデータデスクランブル部32が設けられている。

【0007】図5は、図4に示すDVD-ROMドライブ35の構成図である。図5に示すように、DVD-ROMドライブ35は、データバス55に、RF信号処理部51、RAM52およびマイクロコンピュータ53を接続した構成をしている。また、マイクロコンピュータ53には、認証部40が接続されている。データバス55は、インタフェース42に接続されている。

【0008】以下、DVDディスクから読み出したAVデータを、インタフェース42を介して、AVデコーダ36に出力する際のDVD-ROMドライブ35の動作、いわゆるバス暗号化動作を説明する。図6は、この動作を説明するためのフローチャートである。まず、マイクロコンピュータ53からのサーボ制御に応じてDVDディスクが回転し、光ピックアップ50から、スクランブルされたAVデータ、第1の暗号化されたタイトルキーおよび符号化されたディスクキーが、RF信号処理部51に出力される。これらのデータは、RF信号処理部51において、波形整形などの処理が施された後に、データバス55を介してRAM52に記憶される（ステップS1）。そして、バス動作を開始前に、認証部40において、自らが生成したランダムデータと、図4に示す認証部41からインタフェース42およびマイクロコンピュータ53を介して入力したランダムデータとを用いてバスキーが生成される。認証部40で生成されたランダムデータは、マイクロコンピュータ53およびインタフェース42を介して、認証部41に出力される。そして、AVデコーダ36では、認証部41が生成したランダムデータと、認証部40から入力したランダムデータとを用いて、認証部40で生成したものと同一バスキーが生成される。

【0009】次に、タイトルの再生前に、RAM52に記憶された、第1の暗号化されたタイトルキーが、データバス55を介して、マイクロコンピュータ53に読み出される（ステップS2）。次に、マイクロコンピュータ53に読み出された、第1の暗号化されたタイトルキーが認証部40に出力される（ステップS3）。そして、認証部40において、前述したように生成されたバスキーに基づいて、第1の暗号化されたタイトルキーが、さらに第2の暗号化される（ステップS4）。次に、第2の暗号化されたタイトルキーが、認証部40からマイクロコンピュータ53に読み出される（ステップS5）。次に、マイクロコンピュータ53に読み出された、第2の暗号化されたタイトルキーが、データバス55を介して、RAM52に書き戻される（ステップS6）。

【0010】そして、RAM52に記憶された、スクラ

ンブルされたAVデータと、第2の暗号化されたタイトルキーが、データバス55およびインタフェース42を介して、図4に示すAVデコーダ36に出力される(ステップS7)。次に、AVデコーダ36の認証部41において、前述したバスキーを用いて、第2の暗号化されたタイトルキーが解読され、第1の暗号化されたタイトルキーが生成される。次に、既にディスク挿入時にディスクキー復号部30で復号されたディスクキーを用いて、第1の暗号化されたタイトルキーがタイトルキー解読部31で解読され、当該解読されたタイトルキーを用いて、スクランブルされたAVデータがデスクランブルされ、AVデータが生成される。このAVデータは、例えば、伸長された後に、ディスプレイ33に出力される。

#### 【0011】

【発明が解決しようとする課題】しかしながら、上述した従来のコンピュータ12のDVD-ROMドライブ35では、図6に示すように、RAM52から認証部40への第1の暗号化されたタイトルキーの伝送(ステップS2, S3)、認証部40からRAM52への第2の暗号化されたタイトルキーの伝送(ステップS5, S6)や、ディスクキーの伝送が、マイクロコンピュータ53を介して行われ、マイクロコンピュータ53の処理負担が大きいという問題がある。すなわち、マイクロコンピュータ53では、DVD-ROMドライブ35のサーボ制御の他に、DVD-ROMドライブ35における処理を統括的に制御するが、図6に示すステップS2, S3, S5, S6の処理などが行われる間は、他の制御が待たされてしまい、処理能力が低下するという問題もある。

【0012】本発明は上述した従来技術の問題点に鑑みてなされ、DVD-ROMドライブ装置において、マイクロコンピュータの処理負担を軽減できる記録媒体読み出し装置およびデータ処理装置を提供することを目的とする。

#### 【0013】

【課題を解決するための手段】上述した従来技術の問題点を解決し、上述した目的を達成するために、本発明の記録媒体読み出し装置は、記録媒体に記録された鍵データと当該鍵データによって利用が管理されるコンテンツデータとを読み出し、前記読み出した鍵データを暗号化し、当該暗号化された鍵データを前記読み出したコンテンツデータと共に、インタフェースを介して外部に伝送する記録媒体読み出し装置であって、少なくとも前記記録媒体から前記鍵データおよび前記コンテンツデータを読み出す制御を含む、当該記録媒体読み出し装置における制御を統括的に行う第1の制御手段と、前記読み出した鍵データおよび前記コンテンツデータを記憶する記憶手段と、前記記憶手段に記憶された前記鍵データを暗号化する暗号化手段と、前記記憶手段と前記暗号化手段と

の間の前記鍵データの転送を制御し、前記第1の制御手段とは別個に設けられた第2の制御手段とを有する。

【0014】本発明の記録媒体読み出し装置では、第1の制御手段によるサーボ制御によって回転した記録媒体に記録された鍵データおよびコンテンツデータが第1の記憶手段に読み出される。また、例えば、前記第1の制御手段から第2の制御手段に暗号化処理の開始が指示され、第2の制御手段の制御に基づいて、前記記憶手段に記憶された鍵データが暗号化手段に出力され、当該鍵データが前記暗号化手段にて暗号化される。次に、前記暗号化された鍵データが、前記暗号化手段から前記記憶手段に転送されて記憶される。次に、前記記憶手段に記憶された、前記暗号化された鍵データが、インタフェースを介して外部に出力される。ここで、コンテンツデータは、例えば、ユーザに直接的に提供される画像データやアプリケーションプログラムなどである。

【0015】また、本発明のデータ処理装置は、記録媒体から読み出され、暗号化された鍵データと当該鍵データによって利用が管理されるコンテンツデータとを、インタフェースを介して、記録媒体読み出し装置からデコーダ装置に伝送するデータ処理装置であって、前記記録媒体読み出し装置は、少なくとも前記記録媒体から前記鍵データおよび前記コンテンツデータを読み出す制御を含む、当該記録媒体読み出し装置における制御を統括的に行う第1の制御手段と、前記読み出した鍵データおよび前記コンテンツデータを記憶する記憶手段と、自らが生成した第1のランダムデータと、前記インタフェースを介して前記デコーダ装置から入力した第2のランダムデータに基づいて、前記記憶手段に記憶された前記鍵データを暗号化する暗号化手段と、前記記憶手段と前記暗号化手段との間の前記鍵データの転送を制御し、前記第1の制御手段とは別個に設けられた第2の制御手段とを有する。ここで、前記デコーダ装置は、前記インタフェースを介して前記記録媒体読み出し装置から入力した前記第1のランダムデータと、自らが生成した前記第2のランダムデータとに基づいて、前記インタフェースを介して入力した前記暗号化された鍵データを解読する解読手段と、前記解読された鍵データを用いて、前記インタフェースを介して入力したコンテンツデータを利用可能にするコンテンツデータ処理手段とを有する。

#### 【0016】

【発明の実施の形態】以下、本発明の実施形態に係わる記録媒体読み出し装置としてのDVD-ROMドライブについて説明する。図1は、本実施形態のDVD-ROMドライブ135が用いられるシステムの構成図である。図1において、図4と同じ符号を付したものは、前述したものと同一である。図1に示すように、コンテンツプロバイダ13の一人である著作権所有者200が、著作権の対象となるAVデータ21と、発行したタイトルキー20とをディスク製造者17に供給する。また、

コンテンツプロバイダ13の一人である著作権管理者14が、ディスクキー22を発行し、これをディスクキー管理者15に供給する。ディスクキー管理者15は、ディスクキー22をディスク製造者17のタイトルキー第1の暗号化部18に供給すると共に、ディスクキープロテクション部16において、ディスクキー22を符号化する。この符号化したディスクキー22aは、DVDディスク10に記録される。

【0017】タイトルキー暗号化部18は、ディスクキー22を用いて、タイトルキー20を第1の暗号化し、この第1の暗号化されたタイトルキー20aが、DVDディスク10に記録される。また、AVデータスクランブル部19は、タイトルキー20を用いて、AVデータ21をAVデータスクランブル部19でスクランブル(scramble)する。このスクランブルされたAVデータ21aは、DVDディスク10に記録される。これにより、符号化されたディスクキー22a、第1の暗号化されたタイトルキー20aおよびスクランブルされたAVデータ21aが記録された、DVDディスク10が製造される。

【0018】コンピュータ112は、本発明のデータ処理装置であり、DVD-ROMドライブ135と、AVデコーダ36とを有する。DVD-ROMドライブ135とAVデコーダ36とは、ATAPIあるいはSCSIなどのインタフェース42を介して接続されている。AVデコーダ36は、基本的に、前述した図4に示すものと同じである。

#### 【0019】DVD-ROMドライブ135

DVD-ROMドライブ135は、認証部140を有する。認証部140は、バスキー処理部150および第2の暗号化部151を有する。バスキー処理部150は、バス動作開始前に、自らが生成したランダムデータ172と、インタフェース42を介してバスキー処理部152から入力したランダムデータ170とに基づいて、バスキー171を生成し、このバスキー171を第2の暗号化部151に出力する。

【0020】第2の暗号化部151は、DVDディスク10から読み出された符号化されたディスクキー22aを、DVDディスク10の挿入時に、バスキー171を用いて第2の暗号化し、この第2の暗号化したディスクキー22bを、インタフェース42を介して、AVデコーダ36の第2の解読部153に出力する。また、第2の暗号化部151は、DVDディスク10から読み出された第1の暗号化されたタイトルキー20aを、タイトルの再生時に、バスキー171を用いて第2の暗号化し、この第2の暗号化したタイトルキー20bを、インタフェース42を介して、AVデコーダ36の第2の解読部153に出力する。

【0021】また、DVD-ROMドライブ135は、DVDディスク10から読み出した、スクランブルされ

たAVデータ21aを、インタフェース42を介して、AVデコーダ36のAVデータデスクランブル部32に出力する。

#### 【0022】AVデコーダ36

AVデコーダ36は、認証部41、ディスクキー復号部30、タイトルキー第1の解読部31、AVデータデスクランブル部32およびAVデータ伸長部160を有する。

【0023】認証部41は、バスキー処理部152および第2の解読部153を有する。バスキー処理部152は、インタフェース42を介して、DVD-ROMドライブ135からAVデータ21aを入力する際に、図示しないランダム値発生器によってランダムデータ170を発生し、このランダムデータ170をインタフェース42を介してバスキー処理部150に出力する。また、バスキー処理部152は、インタフェース42を介してバスキー処理部150から入力したランダムデータ172と、ランダムデータ170とに基づいて、バスキー171を生成し、このバスキー171を第2の解読部153に出力する。このとき、バスキー処理部152が生成するバスキー171と、バスキー処理部150が生成するバスキー171とは同じである。

【0024】第2の解読部153は、DVDディスク10の挿入時に、インタフェース42を介して入力した第2の暗号化されたディスクキー22をバスキー171を用いて解読し、符号化されたディスクキー22aを生成する。第2の解読部153は、ディスクキー22aをディスクキー復号部30に出力する。第2の解読部153は、タイトルの再生時に、インタフェース42を介して入力した第2の暗号化されたタイトルキー20bをバスキー171を用いて解読し、第1の暗号化されたタイトルキー20aを生成する。第2の解読部153は、タイトルキー20aをタイトルキー第1の解読部31に出力する。

【0025】ディスクキー復号部30は、符号化されたディスクキー22aを復号してディスクキー22を生成し、これをタイトルキー第1の解読部31に出力する。タイトルキー第1の解読部31は、ディスクキー22を用いて、タイトルキー20aを解読してタイトルキー20を生成し、これをAVデータデスクランブル部32に出力する。AVデータデスクランブル部32は、インタフェース42を介して入力した、スクランブルされたAVデータ21aを、タイトルキー20を用いてデスクランブルしてAVデータ21を生成し、これをAVデータ伸長部160に出力する。AVデータ伸長部160は、圧縮されているAVデータ21を伸長してAVデータを生成し、これをディスプレイに出力する。

【0026】以下、DVD-ROMドライブ135について詳細に説明する。図2は、DVD-ROMドライブ135の構成図である。図2に示すように、DVD-R

OMドライブ135は、認証部140、光ピックアップ50、RF信号処理部51、RAM52、マイクロコンピュータ53およびDMA(Direct Memory Access)部190を有する。図2において、図5と同じ符号を付した構成要素は、前述したものと同一である。図2に示すように、DVD-ROMドライブ135は、データバス55に、認証部140、RF信号処理部51、RAM52およびDMA部190を接続した構成をしている。DMA部190には、マイクロコンピュータ53が接続されている。また、データバス55は、インタフェース42に接続されている。

【0027】DMA部190は、マイクロコンピュータ53が関与しないRAM52へのアクセスを実現し、具体的には、RAM52と認証部140との間でのデータ転送を実現する。以下、DVDディスク10から読み出したAVデータを、インタフェース42を介して、AVデコーダ36に出力する際のDVD-ROMドライブ135の動作を説明する。図3は、この動作を説明するためのフローチャートである。先ず、マイクロコンピュータ53からのサーボ制御に応じてDVDディスクが回転し、光ピックアップ50から、スクランブルされたAVデータ21a、第1の暗号化されたタイトルキー20aおよび符号化されたディスクキー22aが、RF信号処理部51に出力される。これらのデータは、RF信号処理部51において、波形整形などの処理が施された後に、データバス55を介してRAM52に記憶される

(ステップS11)。そして、バス動作を開始前に、認証部140において、自らが生成したランダムデータと、図1に示す認証部41からインタフェース42を介して入力したランダムデータとを用いてバスキーが生成される。認証部140で生成されたランダムデータは、インタフェース42を介して、認証部41に出力される。そして、AVデコーダ36では、認証部41が生成したランダムデータと、認証部140から入力したランダムデータとを用いて、認証部140で生成したものと同一バスキーが生成される。

【0028】また、マイクロコンピュータ53から、DMA部190にバス暗号化動作の開始が指示される(ステップS12)。

【0029】次に、タイトルの再生前に、DMA部190による制御によって、RAM52に記憶された、第1の暗号化されたタイトルキー20aが、データバス55を介して、認証部140に読み出される(ステップS13)。次に、認証部140において、バスキー171に基づいて、第1の暗号化されたタイトルキー20aが、さらに第2の暗号化される(ステップS14)。これによって、第2の暗号化されたタイトルキー20bが生成される。

【0030】次に、DMA190による制御によって、第2の暗号化されたタイトルキー20bが、データバス

55を介して、認証部140からRAM52に読み出される(ステップS15)。すなわち、ステップS13～S15の処理の制御は、マイクロコンピュータ53ではなく、DMA部190によって自動的に行われる。次に、RAM52に記憶された、スクランブルされたAVデータ21aおよび第2の暗号化されたタイトルキー20bが、データバス55およびインタフェース42を介して、AVデコーダ36に出力される(ステップS16)。

【0031】そして、AVデコーダ36では、バスキー処理部152において前記バスキー171を用いて、第2の暗号化部151において、第2の暗号化されたタイトルキー20bが解読され、第1の暗号化されたタイトルキー20aが生成される。この第1の暗号化されたタイトルキー20aはタイトルキー第1の解読部31に出力される。

【0032】タイトルキー第1の解読部31では、ディスク挿入時に既に前述したタイトルキーと同様の過程を経てディスクキー復号部30で復号されたディスクキー22を用いて、第1の暗号化されたタイトルキー20aが解読され、当該解読されたタイトルキー20aがAVデータデスクランブル部32に出力される。AVデータデスクランブル部32では、タイトルキー20を用いて、スクランブルされたAVデータ21aがデスクランブルされ、AVデータ21が生成される。このAVデータ21は、例えば、伸長された後に、ディスプレイ33に出力される。

【0033】以上説明したように、DVD-ROMドライブ135によれば、RAM52と認証部140と間でのタイトルキーおよびディスクキーの転送を、マイクロコンピュータ53による制御ではなく、DMA部190による制御で実現する。そのため、マイクロコンピュータ53は、図3に示すステップS12において、DMA部190にバス暗号化動作の開始を指示した後は、当該バス暗号化処理からは開放され、他の処理を行うことができ、マイクロコンピュータ53の処理負担が軽減される。その結果、マイクロコンピュータ53の処理が高速化される。

【0034】本発明は上述した実施形態には限定されない。上述した実施形態では、記録媒体として、DVDディスクを例示したが、インタフェースを介して記録データを伝送するときに暗号化が要求される規格を持つものであれば特に限定されない。

#### 【0035】

【発明の効果】以上説明したように、本発明の記録媒体読み出し装置およびデータ処理装置によれば、第1の制御手段の処理の負担を軽減できる。

#### 【図面の簡単な説明】

【図1】図1は、本発明の実施形態のDVD-ROMドライブ装置が用いられるシステムの構成図である。



【図2】図2は、図1に示すDVD-ROMドライブの構成図である。

【図3】図3は、DVDディスクから読み出したAVデータを、インタフェース42を介して、AVデコーダ36に出力する際の図2に示すDVD-ROMドライブの動作のフローチャートである。

【図4】図4は、DVDディスクへのディスクキーおよびタイトルキーの記録から、DVDディスクに記録されたAVデータをDVDプレーヤーおよびコンピュータ（DVD-ROMドライブ装置）を用いて再生するまでの過程を説明するための図である。

【図5】図5は、図4に示すDVD-ROMドライブの構成図である。

【図6】図6は、DVDディスクから読み出したAVデータを、インタフェース42を介して、AVデコーダ3

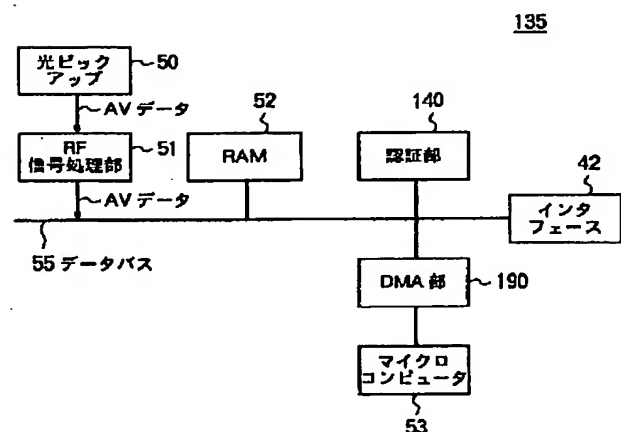
6に出力する際の図5に示すDVD-ROMドライブの動作のフローチャートである。

【符号の説明】

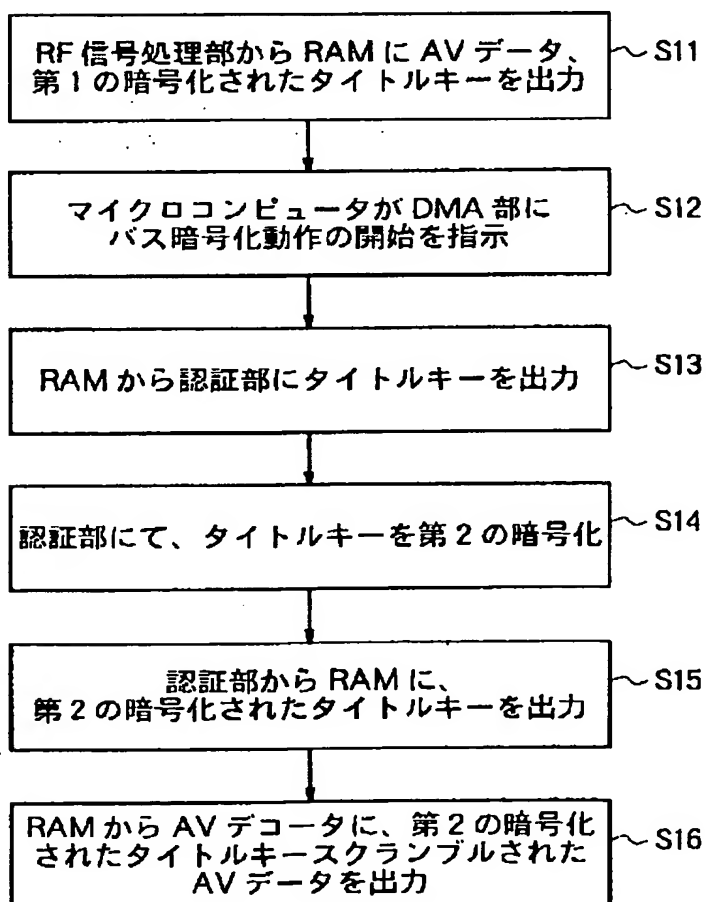
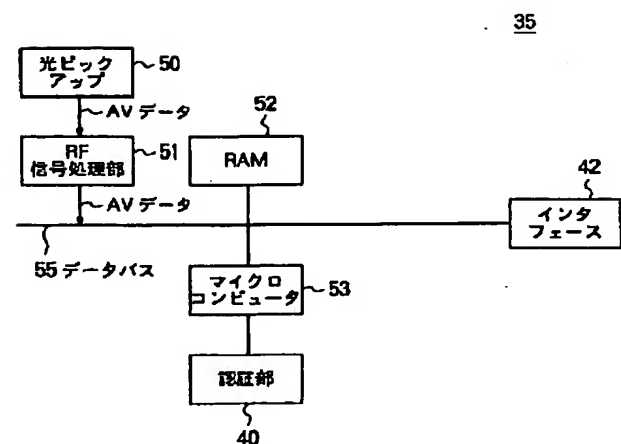
20…タイトルキー、20a…第1の暗号化されたタイトルキー、20b…第2の暗号化されたタイトルキー、21…AVデータ、21a…スクランブルされたAVデータ、22…ディスクキー、22a…符号化されたディスクキー、22b…第2の暗号化されたディスクキー、30…ディスクキー復号部、31…タイトルキー第1の解読部、32…AVデータデスクランブル部、40、41、140…認証部、42…インタフェース（ATAPI）、50…光ピックアップ、51…RF信号処理部、52…RAM、150、152…バスキー処理部、151…第2の暗号化部、153…第2の解読部、160…AVデータ伸長部、190…DMA部

【図2】

【図3】

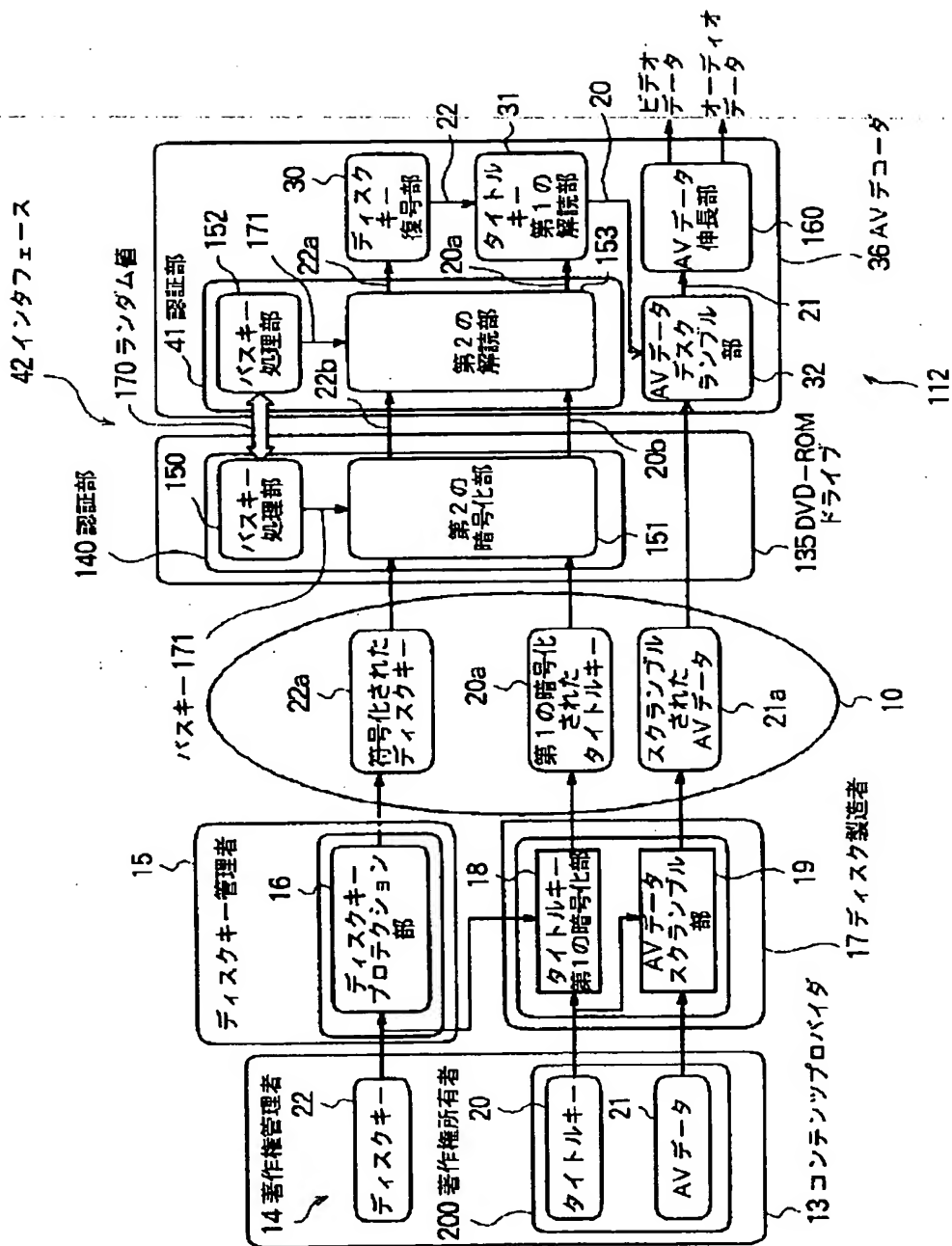


【図5】

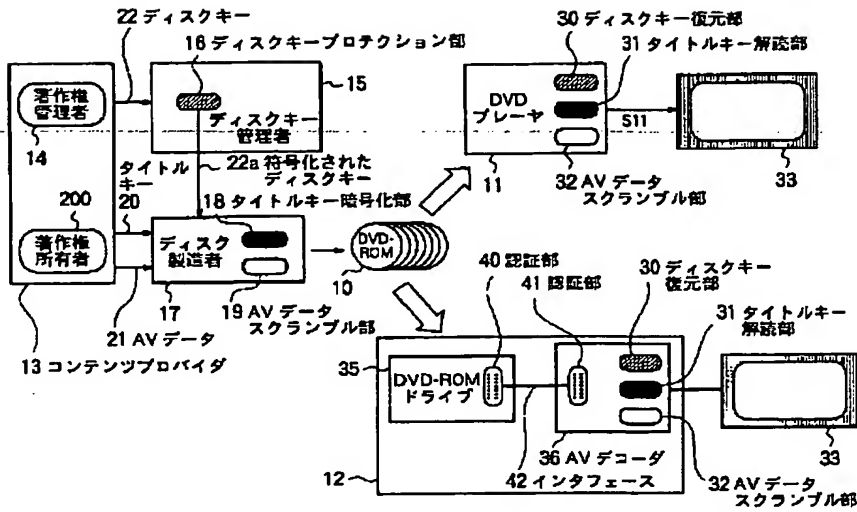




【図1】



【図4】



【図6】

